UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,277	03/06/2002	Ian Curry	10500.02.0123	7718

23418 7590 08/06/2009

VEDDER PRICE P.C.
222 N. LASALLE STREET
CHICAGO, IL 60601

EXAMINER	
PICH, PONNOREAY	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
08/06/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/092,277	CURRY, IAN	
	Examiner	Art Unit	
	PONNOREAY PICH	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 May 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-27 are pending.

Response to Amendment and Arguments

Applicant's amendments submitted on 5/12/09 were fully considered. Any objections or rejections not repeated for record below are withdrawn due to the amendments.

Applicant's arguments submitted on 5/12/09 were also fully considered. As per the response to arguments in the last Office action, applicant pointed out that one cannot get to step 414 in Figure 4A of Perlman by choosing option B. Any confusion caused by the typo is regretted—as applicant notes, it is by choosing option "D" instead of "B" that step 414 is reached. As requested by applicant in the response filed, the examiner attempted to contact the attorney of record before issuing another Office action to clarify matters and to possibly identify subject matter that might lead to an allowance. The examiner waited over a week for a return call from applicant and only issues this Office action without an interview with applicant because the examiner's deadline to process the application has passed while waiting for a return call and the examiner has not been able to reach the attorney of record despite several attempts to do so. Regardless of the typo of pointing to option B instead of D in the last response to argument, the examiner respectfully submits that the currently set of claims rejected based on Perlman's teachings are still valid as the examiner's discussion refers to steps that were clearly taken by choosing option "D" in Figure 4A. Note that applicant always

had the option of calling the examiner for an interview for clarification prior to submitting a response.

Applicant argues that Perlman does not teach receiving an encrypted secret key that is encrypted using a secure distribution server specific public key specific to the secure distribution server. Again, the examiner respectfully disagrees. As pointed out before, Perlman states that the DLE and group server could be combined into one entity if the DLE can be completely trusted (col 6, lines 1-7). As such, steps 406 and 414 as seen in Figure 4A could be combined into one step so that the encrypted message and encrypted message key is sent to the combined DLE/group server entity. The encrypted message key that the DLE/group server entity received as seen in step 404 was encrypted using group public key 107 (col 5, lines 28-32). At step 416, the DLE/group server entity decrypts the encrypted message key using private key 302 to restore the message key (col 5, lines 52-55). Since the message key encrypted using public key 107 is decrypted with private key 302, one can see that public key107 and private key 302 form a public/private key pair. The idea behind the use of a public/private key pair is that the private key is kept secret by the owner of the key pair while anyone can know the public key. The key pair is considered specific to the owner of the key pair—the person who knows the value of the private key. Since the DLE/group server entity decrypted the encrypted message key in step 416 of Figure 4A, one skilled should understand that the limitation being argued is met since public key 107 is a public key specific to the secure distribution server, i.e. the combined DLE/group server entity.

Alternatively, since Perlman did not explicitly come out and say that public key 107 was specific to the DLE/group server, the examiner relied on Graunke's teachings to show that in public key cryptography, the public/private key pair is specific to the sole entity who knows the value of the private key.

Applicant states that Graunke does not contemplate employing a public key pair specific to a secure distribution server nor that an encrypted secret key is encrypted using the secure distribution server. Applicant states that the examiner parsed claim language without taking into account the claim as a whole. The examiner respectfully disagrees. The examiner did not parse the claim language as applicant seems to be arguing and the rejections explained how taking the teachings of both Perlman and Graunke into account, the limitation would have been obvious. The examiner did not rely solely on Graunke's teachings to show what applicant is stating that Graunke does not teach. It is not proper for applicant to view the teachings of the references separately to determine whether or not the claim as a whole is obvious or not. Instead, the teachings of the references together as a whole must be considered. Further, it is not proper to argue against a position that was clearly never taken by the examiner to attempt to overcome the rejections made, see 37 CFR 1.111.

Applicant argues that modifying Perlman using Graunke's teachings would cause Perlman to not be operational since there would be no group public key. The examiner respectfully disagrees. Applicant has not explained how the modification would render Perlman non-operational—group public key 107 would still be in Perlman's invention and at best all Graunke's teachings would do is make it more explicit that since the

private key is known only to the DLE/group server, group public key 107 is therefore specific to the DLE/group server. Argument by applicant alone is not evidence.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 6-7, 10, 12, 15-24, and 26 are rejected under 35 U.S.C. 102(e) as anticipated by Perlman et al (US 6,912,656) as evidenced by Graunke et al (US 5,991,399) or, in the alternative, under 35 U.S.C. 103(a) as obvious over Perlman et al (US 6,912,656) in view of Graunke et al (US 5,991,399).

Claims 1, 15, 18, and 20:

As per claim 1, Perlman discloses:

1. Receiving encrypted information (i.e. encrypted message 210) from a sender for transmission to at least one intended recipient (col 5, lines 10-12 and 25-37) and receiving an encrypted secret key (i.e. encrypted message key 210) encrypted using a secure distribution server specific public key (i.e. public key 107) of a public/private key pair specific to the secure distribution server (col 5, lines 28-30 and 52-55). *Note that encrypted message key 210 was encrypted using public key 107. The group server 114 decrypts encrypted message key 210 using private key 302 (col 5, lines 32-34 and 53-55). This means that public key 107 and private key 302 are a public/private key pair. Since private key 302 corresponds to group server 114 (col 5, lines 5-10), public key 107 also corresponds to group server 114. The examiner considers the combination of the DLE and the group server as the claimed secure distribution server. Note that Perlman discloses that the DLE forwards messages (col 5, lines 34-37) while the group server decrypts the encrypted message key (col 5, lines 48-55). Perlman discloses that rather than use a separate group server, the functionalities of the DLE and group server could be incorporated into the DLE (col 6, lines 1-5). The public key 107 and private key 302 are specific to the secure distribution server (i.e. DLE/group server) because in Figure 4A, if options A, D, and E were chosen, the embodiment of Perlman's invention is such that the DLE/group server is the only entity to know the value of the group private key 302. To send the message key to the recipients, in step 418, the message key is*

re-encrypted with a different public key that is specific to the recipient (col 6, lines 56-65).

2. Decrypting the encrypted secret key to produce a decrypted secret key (col 5, lines 52-54).
3. Obtaining a corresponding public key of at least one intended recipient (Fig 3 and col 5, lines 55-60).
4. Encrypting the decrypted secret key for the at least one intended recipient using a corresponding pubic key specific to the at least one intended recipient to produce at least one recipient specific secure secret key (Fig 3; Fig 4A, step 418; col 2, lines 60-65; and col 5, lines 55-60 and 65-67). *Note that after the group server decrypts encrypted message key 210, it re-encrypts the message key for transmission to at least one recipient. In column 5, lines 55-60, Perlman discloses that in his invention a variety of key types could be utilized to encrypt the decrypted secret message key. One of these key types is a public key 312 belonging/specific to at least one recipient. Encrypted message key 308 is formed from the encryption of the message key using public key 312 of the recipient (step 418 in Figure 4A).*
5. Forwarding the encrypted information sent by the sender and at least one recipient specific secure secret key for the at least one intended recipient (col 5, lines 14-15, 34-37, and 65-66).

As evidenced by Graunke, in public key cryptography systems two keys are used for cryptographic operations, where the public key is public and the corresponding private key is known only to the particular user/entity (col 1, lines 50-56). Note that public key 107 and private key 302 disclosed by Perlman forms a key pair where the public key 107 is used by sender 104 to encrypt message key 204 while private key 302 is used by the group server 114 to decrypt the received encrypted message key (Fig 4A, steps 404 and 416 and col 5, lines 23-55). While the public/private key disclosed by Perlman is associated with a group of valid recipients, in one embodiment of Perlman's invention which utilizes options B and E in Figure 4A, no entity other than the group server 114 knows the value of the private key 302. As such, public key 107 and private key 302 can be considered as belonging only to and being specific to group server 114, thus the public key 107 disclosed by Perlman can be considered a secure distribution server specific public key of a public/private key pair specific to the secure distribution server because as evidenced by Graunke's teachings, in public/private key cryptography, the key pair is owned by and is specific only to a particular user (col 1, lines 50-56).

Alternatively, assuming for the sake of argument, that even if in Perlman's both public key107 and private key 302 could conceivably be known by/owned by some other entity other than group server 107, it would have been obvious to one skilled in the art to modify Perlman's invention such that public key 107 and private key 302 was only known by/owned by group server 107 by making group server 107 the only entity to know the value of private key 302 as per Graunke's teachings, thus making public key

107 a "secure distribution server specific public key of a public/private key pair specific to the secure distribution server". One skilled would have been motivated to do so because Graunke teaches that in public key cryptography, the private key is only known to a particular user (col 1, lines 50-56). Further, one skilled in the art should appreciate that decreasing the number of entities that know the value of the private key would increase security since there is less chances of the key value being discovered.

Claim 15 recites a method similar to claim 1 and is rejected for substantially similar reasons. The difference is that claim 15 recites that each of the steps of the method recited in claim 1 is done by a secure distribution server. As explained above, the examiner considers the combination of the DLE and group server disclosed by Perlman as the claimed secure distribution server. Because each of the above steps discussed above as anticipated by Perlman are performed by the DLE and/or group server of Perlman, Perlman also anticipates the method of claim 15.

Claim 18 is directed to a network element comprising one or more processing devices operative to perform the method of claim 1. Claim 18 is rejected for much the same reasons as claim 1. The DLE/group server of Perlman is considered the one or more processing devices referred to in claim 18.

Claim 20 is directed towards a computer storage medium comprising memory containing executable instructions that when read by one or more processing devices causes the one or more processing devices to perform the method of claim 1. Claim 20 is rejected for much the same reasons as claim 1. Note that Perlman's invention is implemented using a network of computer systems (Fig 1), thus a computer storage

medium comprising memory containing executable instructions is inherent to his invention.

Claim 24:

Perlman discloses:

1. At least one sender (i.e. Fig 1, sender 104) that encrypts information (i.e. message 105) with a secret key (i.e. message key 204) to produce encrypted information (i.e. encrypted message 206), encrypts the secret key with a public key (i.e. public key 107) associated with a secure distribution server specific public key of a public/private key pair specific to the secure distribution server associated with a network element (Fig 4A, step 404) to produce an encrypted secret key (i.e. encrypted message key 210), and during an online session, sends the encrypted information and the encrypted secret key to the network element (col 5, lines 10-37 and 48-55). *Public key 107 and private key 302 form a public/private key pair (col 5, lines 32-34). Since private key 302 corresponds to group server 114, public key 107 also corresponds to the DLE/group server entity that the examiner is considering the recited secure distribution server associated with a network element. The public key 107 and private key 302 are specific to the secure distribution server (i.e. DLE/group server) because in Figure 4A, if options A and E were chosen, the embodiment of Perlman's invention is such that the DLE/group server is the only entity to know the value of the group private key 302. To send the message key to the recipients, in step*

418, the message key is re-encrypted with a different public key that is specific to the recipient (col 6, lines 56-65).

2. At least one intended recipient (Fig 1, recipients 106 and 108).
3. At least one network element (i.e. the combination of DLE 110 and group server 114), operatively coupled to the sender at least one intended recipient (Fig 1 and col 6, lines 1-5), including one or more processing devices operative to:
    a. Decrypt the encrypted secret key to produce a decrypted secret key (col 5, lines 52-54).
    b. Obtaining a corresponding public key of at least one intended recipient (Fig 3 and col 5, lines 55-60).
    c. Encrypt the decrypted secret key for the at least one intended recipient using a corresponding pubic key specific to the at least one intended recipient to produce at least one recipient specific secure secret key (Fig 3; col 2, lines 60-65; and col 5, lines 55-60 and 65-67). *Note that after the group server decrypts encrypted message key 210, it re-encrypts the message key for transmission to at least one recipient. In column 5, lines 55-60, Perlman discloses that in his invention a variety of key types could be utilized to encrypt the decrypted secret message key. One of these key types is a public key 312 belonging/specific to at least one recipient. Encrypted message key 308 is formed from the encryption of the message key using public key 312 of the recipient.*

d. Forward the encrypted information sent by the sender and at least one recipient specific secure secret key for the at least one intended recipient (col 5, lines 14-15, 34-37, and 65-66).

As evidenced by Graunke, in public key cryptography systems two keys are used for cryptographic operations, where the public key is public and the corresponding private key is known only to the particular user/entity (col 1, lines 50-56). Note that public key 107 and private key 302 disclosed by Perlman forms a key pair where the public key 107 is used by sender 104 to encrypt message key 204 while private key 302 is used by the group server 114 to decrypt the received encrypted message key (Fig 4A, steps 404 and 416 and col 5, lines 23-55). While the public/private key disclosed by Perlman is associated with a group of valid recipients, in one embodiment of Perlman's invention which utilizes options D and E in Figure 4A, no entity other than the group server 114 knows the value of the private key 302. As such, public key 107 and private key 302 can be considered as belonging only to and being specific to group server 114, thus the public key 107 disclosed by Perlman can be considered a secure distribution server specific public key of a public/private key pair specific to the secure distribution server because as evidenced by Graunke's teachings, in public/private key cryptography, the key pair is owned by and is specific only to a particular user (col 1, lines 50-56).

Alternatively, even if in Perlman's both public key107 and private key 302 could conceivably be known by/owned by some other entity other than group server 107, it

would have been obvious to one skilled in the art to modify Perlman's invention such that public key 107 and private key 302 was only known by/owned by group server 107 by making group server 107 the only entity to know the value of private key 302 as per Graunke's teachings, thus making public key 107 a "secure distribution server specific public key of a public/private key pair specific to the secure distribution server". One skilled would have been motivated to do so because Graunke teaches that in public key cryptography, the private key is only known to a particular user (col 1, lines 50-56). Further, one skilled in the art should appreciate that decreasing the number of entities that know the value of the private key would increase security since there is less chances of the key value being discovered.

Claims 2, 16, and 21:

Perlman further discloses determining a plurality of intended recipients and retrieving corresponding public keys of the plurality of intended recipients for encrypting the decrypted secret key (col 5, lines 10-18 and 53-60).

Perlman discloses of at a plurality of intended recipients, i.e. recipient 106 and 108. Note that in a public/private key system, the private key is kept secret by the owner of the public/private key pair. This implies that each recipient have its own corresponding public/private key pair. When the DLE/group server re-encrypts the message key for each recipient using each recipient's corresponding public key to form encrypted message key 308, the corresponding public key of the plurality of intended recipients has to be retrieved by the DLE/group server for encrypting the decrypted secret/message key.

Claims 3, 17, and 22:

Perlman further discloses the step of encrypting the decrypted secret key with a corresponding public key of the at least one intended recipient includes encrypting a copy of the decrypted secret key for each intended recipient with a corresponding recipient public key (col 5, lines 16-18 and 53-60).

Claim 4:

Perlman further discloses encrypting information with the secret key to produce the encrypted information (col 5, lines 25-26), encrypting the secret key with the secure distribution server specific public key of the secure distribution server to produce the encrypted secret key (col 5, lines 28-32 and 53-60 and Figure 4A, steps 404 and 416), and sending the encrypted information and the encrypted secret key to the secure distribution server (col 5, lines 34-37). The public key disclosed by Perlman used to encrypt the secret key being the specific to the secure distribution server is evidenced by/made obvious by Graunke's teachings as discussed above.

Claim 6:

The limitation of storing the encrypted information locally on a device that performed the step of encrypting information with the secret key is inherent to Perlman's invention. To be able to encrypt and then forward the encrypted information/message to the secure distribution server (i.e. the DLE/group server), the device which performed the encryption process must store the encrypted information locally in memory before being able to send the encrypted information.

Claim 7:

Perlman further discloses encrypting the secret key, by a sending device, with a public key associated with at least one of a user of the sending device and the sending device (col 5, lines 28-30 and Fig 2).

Claims 10 and 23:

As per claim 10, Perlman further discloses of determining by the secure distribution server, if the encrypted information needs to be sent to other entities, if so, encrypting the decrypted secret key using a public key associated with each of the additional entities (col 3, lines 45-48; col 5, lines 12-15, 48-48-60; and col 6, lines 1-5).

Note that the message could be intended for multiple recipients, thus the public key of each of the recipients would have to be utilized to encrypt the secret/message key so that the encrypted message key could be sent to each of the recipients.

Claim 23 recite limitations substantially similar to what is recited in claim 10 and is rejected for similar reasons.

Claims 12, 19, and 26:

As per claim 12, Perlman further discloses wherein retrieving the corresponding public keys of the plurality of intended recipients for encrypting the decrypted secret key includes obtaining the corresponding public keys from at least one of: a certificate retrieval and validation service, an LDAP lookup and a certificate directory lookup (col 5, lines 52-58 and 61-65 and col 7, lines 13-28).

Claim 19 is directed to the one or more processing devices performing the method of claim 12, thus is rejected for similar reasons as claim 12.

Claim 26 is directed to the network element performing the method of claim 12, thus is rejected for similar reasons as claim 12.

Claims 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al (US 6,912,656) as evidenced by/in view of Graunke et al (US 5,991,399) in further view of Leigh (US 7,284,067).

Claim 5:

Perlman discloses encrypting the secret key using a public key for a secure distribution server to produce a secure distribution server specific encrypted secret key (col 5, lines 28-32 and 52-55). Perlman does not explicitly disclose the encrypting is done using a public key for each of a plurality of secure distribution servers which produces a plurality of secure distribution server specific encrypted secret keys.

However, Leigh discloses that at the time applicant's invention was made, it was known in the art that it was desirable to connect multiple servers to a network for purposes of load balancing (col 1, lines 22-24).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Perlman's invention such that rather than have one secure distribution server (i.e. DLE/group server), there were a plurality of secure distribution servers (as per Leigh's teachings). One skilled would recognize that because there are multiple secure distribution servers in the combination invention of Perlman and Leigh, the sender would then need to encrypt the secret key using the public key for each of

the plurality of secure distribution servers to produce a plurality of secure distribution server specific encrypted secret keys. One skilled would have been motivated to modify Perlman's teachings in the manner discussed because it would prevent overburdening of Perlman's DLE/group server and because it would provide for network redundancy, which would allow messages to be sent even if some of the distribution servers went offline for whatever reason.

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al (US 6,912,656) as evidenced by/in view of Graunke et al (US 5,991,399) in further view of Ofir (US 2003/0007645).

Claim 8:

Perlman does not explicitly disclose digitally signing the information using a private signing key associated with at least one of a user of a sending device and the sending device. However, Ofir discloses a message being signed with a sender's private key (paragraph 38). At the time applicant's invention was made, it would have been obvious to one skilled in the art in light of Ofir's teachings to modify Perlman's invention such that the information sent from the sender to the DLE/group server was digitally signed using a private signing key associated with at least one of a user of a sending device and the sending device. One skilled would have been motivated to do so because it would enable the recipient to authenticate the message as being sent by

the sender (Ofir: paragraph 38). Being able to authenticate the identity of the sender of a message was a well known goal in field network communication.

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al (US 6,912,656) as evidenced by/in view of Graunke et al (US 5,991,399) in further view of Gehring (US 2002/0116606).

Claim 9:

Perlman discloses the encrypted information and the encrypted secret key being sent by the sender (col 5, lines 34-37). Perlman does not explicitly disclose receiving the encrypted information and the encrypted secret key and forwarding the encrypted information and the encrypted secret key to the secure distribution server without decrypting the encrypted secret key.

However, note that Perlman's invention is practiced in a network environment (Fig 1). Gehring discloses in paragraph 5 that in networks consisting of multiple interconnected nodes (i.e. such as the one disclosed by Perlman in Figure 1), some nodes cannot communicate directly with each other. In these cases, it was known in the art that some nodes acted as relays that forwarded messages between nodes that cannot communicate directly with each other. In these known prior art networks, Gehring discloses that the forwarding nodes receives an encrypted message and forwards the encrypted message to its destination without decrypting the encrypted message (paragraph 6). Recall that in Perlman's invention, the message sent from the

sender to the receiver is a bundle 212 consisting of the encrypted message/information and the encrypted secret/message key (col 5, lines 34-37).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Perlman's invention such that it contained one or more forwarding nodes which Gehring disclosed was well known in the prior art such that the forwarding nodes received the encrypted information and the encrypted secret key and forwards the encrypted information and the encrypted secret key to the secure distribution server without decrypting the encrypted secret key. The rationale for why it would have been obvious to one skilled in the art is that networks such as the one utilized by Perlman to practice his invention typically contain several nodes which cannot communicate directly with each other, thus requires relay nodes to forward messages. Perlman's invention as disclosed by him is a system ready for improvement (i.e. needing relay nodes) and the use of the known relaying technique as discussed by Gehring does no more than yield the predictable result of having nodes in the network which relays bundle 212 from the sender to the DLE/group server without decrypting the bundle.

Claims 11 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al (US 6,912,656) as evidenced by/in view of Graunke et al (US 5,991,399) in further view of Chen et al (US 5,832,208).

Claims 11 and 27:

As per claim 11, Perlman discloses the steps of: encrypting the decrypted secret key using a public key and sending the encrypted information and the encrypted secret key.

Perlman does not explicitly disclose the public key is associated with a content scanning device; the sending is to the content scanning device; receiving a result back from the content scanning device, forwarding the encrypted information based on the result sent by the content scanning device and based on at least one recipient specific secure secret key for at least one intended recipient.

However, Chen discloses a virus scanner, i.e. content scanning device, being implemented on a server (col 5, lines 53-60). Chen discloses that emails sent to the server are scanned for viruses, an alert is generated if a virus is detected, and if possible, the virus is removed from the email attachment (col 5, lines 25-27 and col 7, lines 57-60).

In light of Chen's teachings, it would have been obvious to one of ordinary skill in the art to have combined Perlman and Chen's teachings according to the limitations recited in claim 11. One of ordinary skill would have been motivated to do so as scanning messages for viruses and removing the virus from email messages would prevent the spread of viruses to recipients of the email messages, which would compromise the recipient's system and any network they are attached to.

Claim 27 recites a network element which performs the limitations of the method recited in claim 11 and is rejected for the same reasons given in claim 11. Note the

public keying of Perlman being the "non-group public key" is evidenced by/made obvious by Graunke's teachings as discussed above.

Claims 13 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al (US 6,912,656) as evidenced by/in view of Graunke et al (US 5,991,399).

Claims 13 and 25:

As per claim 13, Perlman further discloses encrypting information with the secret key to produce the encrypted information (col 5, lines 25-26), encrypting the secret key with the public key of the secure distribution server to produce the encrypted secret key (col 5, lines 28-32 and 53-60), and during an on line session, sending the encrypted information and the encrypted secret key to the secure distribution server (col 5, lines 34-37.

Perlman does not explicitly disclose the encryption of the information and secret key are done offline. However, the examiner submits that encrypting information and a secret key offline was well known in the art. For example, it is well known that a user can prepare an email message for sending on a laptop when the laptop does not have a network connection, i.e. if the user was on a plane for a business trip. The message is usually prepared to a state where the only thing needed to be able to send the email is a network connection. Later, when the laptop is connected to a network, the message can then be sent. It would have been obvious to have the encryption of the message

and key done offline prior to connecting to a network as the encryption process might take a long time and connection charges on the road can be expensive.

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Perlman's invention according to the limitations recited in claim 13. The rationale for why it would have been obvious to one skilled in the art to modify Perlman's invention according to the limitations recited in claim 13 is that the application of the known technique of encrypting data while offline for later transmission during an online session would do no more than yield a predictable result of allowing Perlman's sender to encrypt information and the secret key while offline, which would allow Perlman's sender to prepare a message for sending even when not online. The public key of Perlman being the "non-group public key" is evidenced by/made obvious by Graunke's teachings as discussed above.

Claim 25 recites a similar limitation as claim 13 and is rejected for similar reasons.

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al (US 6,912,656) as evidenced by/in view of Graunke et al (US 5,991,399) in further view of Bouchard et al (US 2002/0091928).

Claim 14:

Perlman does not disclose sending the encrypted information to a time stamper and receiving a time stamped result prior to forwarding the encrypted information and the at least one recipient specific secure secret key to the at least one corresponding intended recipient.

However, Bouchard discloses time stamping a message by a time stamper prior to forwarding the message to a recipient (p3, paragraph 31, lines 11-15 and Fig 2). In light of Bouchard's teachings it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made modify Perlman's invention according to the limitations recited in claim 14. One of ordinary skill would have been motivated to do so as Bouchard discloses that applying a time stamp to a message allow for an audit log of the message, which is useful in preventing the repudiation of digitally-signed documents/messages (p3, paragraph 28).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PONNOREAY PICH whose telephone number is (571)272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ponnoreay Pich/
Primary Examiner, Art Unit 2435